УДК 519.719.2

М.А. ГРИШИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ОБЗОР МЕТОДОВ И ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ФАЗЗИНГ-ТЕСТИРОВАНИЯ РЕАЛИЗАЦИЙ КРИПТОГРАФИЧЕСКИХ БИБЛИОТЕК

Работа посвящена исследованию подходов инструментальной и технологической поддержки автоматизированного выявления ошибок и уязвимостей в реализациях криптографических библиотек с применением техники фаззинга. Проведена классификация существующих фаззеров, реализуемых ими схем тестирования применительно к криптографическим функциям и протоколам, а также их сравнительный анализ. В результате проведенного анализа выявлен ряд недостатков в существующих релевантных фаззинг-системах и предложены перспективные направления их развития.

Криптографические алгоритмы играют ключевую роль в обеспечении информационной безопасности современных компьютерных систем. Дефекты в их реализациях способны привести к возникновению уязвимостей, снижающих устойчивость системы к угрозам, поэтому своевременное обнаружение и ликвидация ошибок становится приоритетной задачей. Фаззинг - техника автоматизированного выявления уязвимостей посредством подачи некорректных либо частично корректных данных на вход тестируемого ПО [1]. В то же время сложность архитектуры криптографических алгоритмов и специфика требований к обработке входных данных обуславливают потребность в разработке специализированных инструментальных средств, направленных на повышение эффективности и точности фаззинг-тестирования.

В табл. 1 представлен обзор распространенных инструментальных средств (ИС) и применяемых ими методов обнаружения ошибок, среди которых отдельно можно выделить:

1) *метод дифференциального тестирования* – в общем случае заключается в проверке принадлежности значения некоторой функции $\boldsymbol{f}(\boldsymbol{p_1}(\boldsymbol{x}), \dots, \boldsymbol{p_n}(\boldsymbol{x}))$ критической области, где $\boldsymbol{p_1}, \dots, \boldsymbol{p_n}$ – разные реализации одного алгоритма. В базовом случае проверяется $\boldsymbol{p_1}(\boldsymbol{x}) = \boldsymbol{p_2}(\boldsymbol{x})$;

2) *метод кросс-проверок* – выявление логической неконсистентности в результатах применения композиции функций одной реализации $\boldsymbol{p}$ $\boldsymbol{Verify}\left(\boldsymbol{f_p^1}\circ \ldots \circ \boldsymbol{f_p^n}(\boldsymbol{x})\right) \in \{\mathbf{0},\mathbf{1}\}$;

3) *семантический метод* – генерация семантически корректных тестовых наборов с целью обхода множества проверок в реализациях.

Таблица 1. Распространенные методы фаззинга криптографических библиотек

ИС	Классификация	Цель	Типы ошибок	Методы
CDF	Генерационный, черный ящик	Реализации базовых примитивов (функции в OpenSSL, SymCrypt, wolfCrypt и т.д.)	ошибки логики реализации; утечки времени	дифференциальное тестирование; кросс-проверки
Cryptofuzz	Комбинированный, серый ящик		ошибки работы с памятью; ошибки логики реализации	дифференциальное тестирование; кросс-проверки;
CLFuzz	Мутационный, серый ящик		ошибки логики реализации; ошибки работы с памятью; архитектурные ошибки	семантический метод; дифференциальное тестирование; кросс-проверки;
Tls-fuzzer dtls-fuzzer	Генерационный, черный ящик	TLS/DTLS/SSL реализации (клиент / сервер)	отклонения от спецификаций; ошибки памяти в парсерах сообщений; нарушение последовательности сообщений в handshake	стресс-метод; сценарный метод

На основе проведенного анализа можно предложить следующие возможные направления модификации фаззинг-схем тестирования криптографических библиотек:

1) расширение множества проверяемых фаззером криптографических свойств, в частности, с помощью интеграции с релевантными сканнерами, переход к отслеживанию многофакторных состояний;

2) построение распределенной системы тестирования с выделенными фаззинг-кластерами, отвечающими за поиск отдельных классов ошибок, для повышения отказоустойчивости и ускорения анализа;

3) разработка и применение адаптивных биомимикрических алгоритмов в семантико-ориентированном фаззинге как альтернативы случайному выбору операторов мутации.

Список литературы

1. ГОСТ Р 56939-2024 Защита информации. Разработка безопасного программного обеспечения. Общие требования. М.: Стандартинформ, 2024. – 120 с. – Утверждён приказом Росстандарта от 24.10.2024 № 1504-ст.